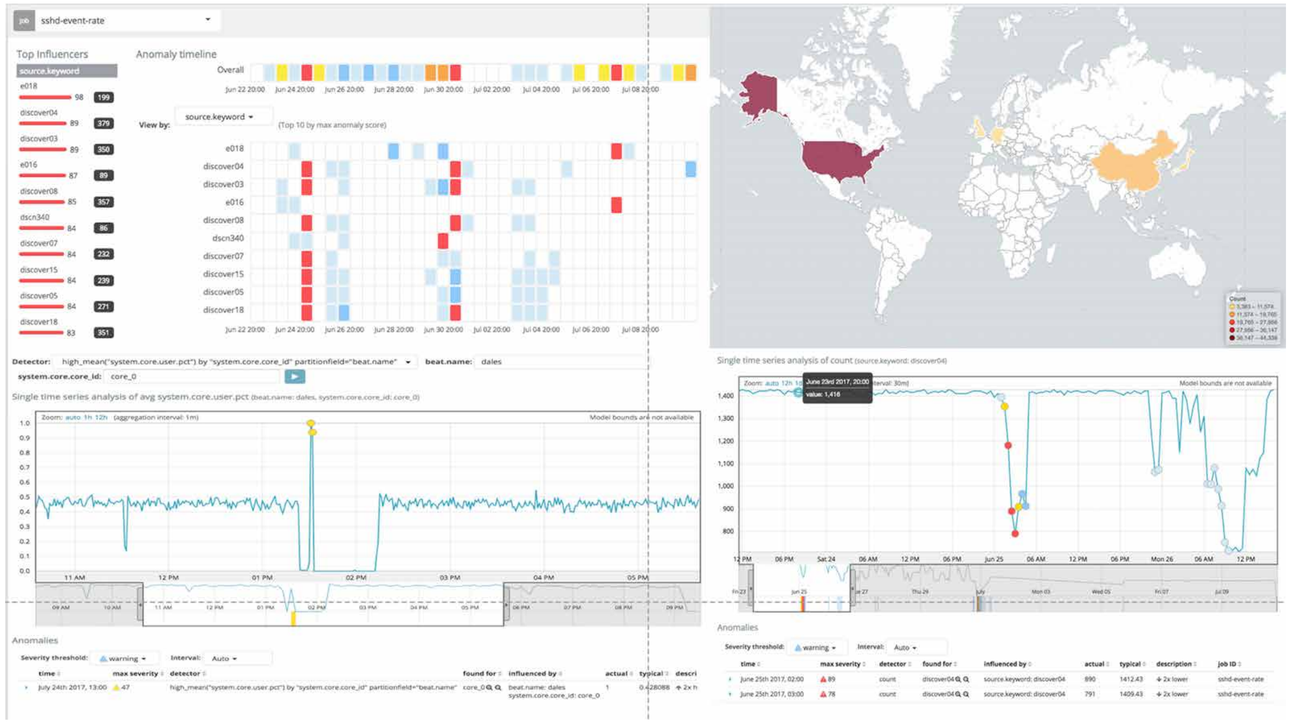
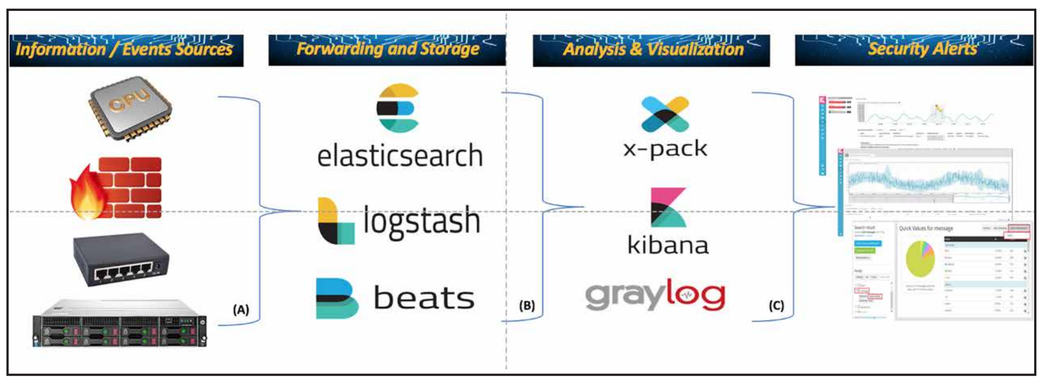


Kibana dashboards represent multiple advanced machine learning jobs. The graphs cover connection event rate, user authentication, and real-time system usage statistics. The data came from multiple NASA Center for Climate Simulation (NCCS) production systems and was filtered and ingested with Logstash and Metricbeat. Red to yellow squares and dots represent possible anomalies found with their date and time. X-Pack machine learning (ML) features classify anomalies according to confidence based on the model baseline. *Jordan A. Caraballo-Vega, Jasaun J. Neff, NASA/Goddard*



Workflow of our ML SIEM infrastructure. Log data from systems (A)–CPU metrics, firewalls, switches, servers, and others–are parsed and stored in a log storage cluster (B). After messages are indexed, they are analyzed through ML models where analysis functions like mean, sum, and many others are calculated to identify deviations from baseline values and their influencers. Results can be visualized in dashboards (C) including real-time graphs and specific anomaly information.
Jordan A. Caraballo-Vega, Jasaun J. Neff, NASA/Goddard

National Aeronautics and
Space Administration

Cybersecurity Machine Learning

The NASA Center for Climate Simulation (NCCS) currently monitors and stores logs from thousands of assets and a wide variety of services. In order to enhance and improve our ability to view, analyze, and monitor our systems, we implemented unsupervised machine learning techniques and a security information and event management (SIEM) infrastructure for detecting anomalies.

We built an ELK (Elasticsearch, Logstash, Kibana) + X-Pack infrastructure to filter and ingest data and analyze it with machine learning models in combination with Kibana dashboards and other ELK resources. Machine learning was highly effective and useful for analyzing real-time and archived data and will emerge as a powerful analytics technique for log analysis and a great engine for SIEM.

Jordan A. Caraballo-Vega, NASA Goddard Space Flight Center
Jasaun J. Neff, NASA Goddard Space Flight Center